IN THE CLAIMS

Please amend the claims as follows:

1-36. (Canceled)

37. (Currently Amended) A method of a media verification system for identifying recording media, comprising:

generating, by a data processing device of the media verification system, a plurality of different signature data elements from a secret key data element, [[and]] a message data element and a variable, where the message data is a generator of a cyclic group for a title of an encrypted content;

generating, by the data processing device, a plurality of different identification data elements, each of the plurality of different identification data elements including a generated signature data element of the plurality of different signature data elements and the message data element used in the generating of the generated signature data elements, and storing the plurality of different identification data elements in an electronic memory of the media verification system;

assigning one of the plurality of generated identification data elements to each of a plurality of different recording media;

recording, by a media writing device of the media verification system, one of the plurality of generated identification data elements to an assigned recording media;

generating a verification data element from the generated signature data element of the identification data element recorded on the assigned recording media using a public key;

comparing, by the data processing device, the verification data element to the message data element of the identification data element recorded on the assigned recording media to determine whether the verification data element and the message data element of the

identification data element recorded on the assigned recording media are the same, and verifying the identification data element based upon a determination that the verification data element is the same as the message data element of the identification data recorded on the assigned recording media; and

writing, by a media recording device, [[an]] the encrypted content to the assigned recording media based upon a determination that the assigned recording media is verified in the comparing, wherein the media recording device is configured to inhibit writing the encrypted content to a recording media having an unverified identification data element or no identification data element recorded thereon.

38. (Previously Presented) The method according to Claim 37, further comprising:

generating an identification revocation list, wherein the identification revocation list includes an identification data element corresponding to an unauthorized recording media; and

recording the identification revocation list to the assigned recording media using the media writing device, wherein

the media recording device is further configured to inhibit writing the encrypted content to the assigned recording media based upon a determination that the identification data element recorded on the assigned recording media is included in the identification revocation list.

39. (Currently Amended) A computer readable medium including computer executable instructions, wherein the instructions, when executed by a data processing device, cause the data processing device to perform a method for generating identification data for identifying recording media, the method comprising:

generating a plurality of different signature data elements from a secret key data element, [[and]] a message data element and a variable using a data processing device, where the message data is a generator of a cyclic group for a title of an encrypted content;

generating a plurality of different identification data elements using the data processing device, each of the plurality of different identification data elements including a generated signature data element of the plurality of different signature data elements and the message data used in the generating of the generated signature data elements, and storing the plurality of different identification data elements in an electronic memory;

assigning one of the plurality of generated identification data elements to each of a plurality of different recording media;

recording one of the plurality of generated identification data elements to an assigned recording media using a media writing device;

generating a verification data element from the generated signature data element of the identification data element recorded on the assigned recording media using a public key;

comparing the verification data element to the message data element of the identification data element recorded on the assigned recording media using the data processing device to determine whether the verification data element and the message data element of the identification data element recorded on the assigned recording media are the same, and verifying the identification data element based upon a determination that the verification data element is the same as the message data element of the identification data element recorded on the assigned recording media; and

writing [[an]] the encrypted content to the assigned recording media using a media recording device based upon a determination that the assigned recording media is verified in the comparing, wherein the media recording device is configured to inhibit writing the

encrypted content to a recording media having an unverified identification data element or no identification data element recorded thereon.

40. (Previously Presented) The computer readable medium according to Claim 39, the method further comprising:

generating an identification revocation list, wherein the identification revocation list includes an identification data element corresponding to an unauthorized recording media; and

recording the identification revocation list to the assigned recording media using the media writing device, wherein

the media recording device is further configured to inhibit writing the encrypted content to the assigned recording media based upon a determination that the identification data element recorded on the assigned recording media is included in the identification revocation list.

41. (Currently Amended) A media verification system for identifying recording media, comprising:

a data processing device configured to

generate a plurality of different signature data elements from a secret key data element, [[and]] a message data element and a variable, where the message data is a generator of a cyclic group for a title of an encrypted content,

generate a plurality of different identification data elements, wherein each of the plurality of different identification data elements includes a generated signature data element of the plurality of different signature data elements and the message data element used in generating of the generated signature data elements,

store the plurality of different identification data elements in an electronic memory, and

assign one of the plurality of generated identification data elements to each of a plurality of different recording media;

a media writing device configured to record one of the plurality of generated identification data elements to an assigned recording media;

a data processing device configured to generate a verification data element from the generated signature data element of the identification data element recorded on the assigned recording media using a public key;

a comparison device configured to compare the verification data element to the message data element of the identification data element recorded on the assigned recording media and verify the identification data element based upon a determination that the verification data element is the same as the message data element of the identification data element recorded on the assigned recording media; and

a media recording device configured to record [[an]] the encrypted content to the assigned recording media based upon a determination that the assigned recording media is verified by the comparison device, and the media recording device is further configured to inhibit writing the encrypted content to a recording media having an unverified identification data element or no identification data element recorded thereon.

42. (Previously Presented) The media verification system according to Claim 41, further comprising:

a data processing device configured to generate an identification revocation list, wherein the identification revocation list includes an identification data element corresponding to an unauthorized recording media; and

a media writing device configured to record the identification revocation list to the assigned recording media, wherein

the media recording device is further configured to inhibit writing the encrypted content to the assigned recording media based upon a determination that the identification data element recorded on the assigned recording media is included in the identification revocation list.

43. (Previously Presented) The method according to Claim 37, wherein the different signature data elements are generated from the secret key data element, the message data element and a different integer selected from a set having a number of integers equal to a number of the different recording media.

44. (Previously Presented) The computer readable medium according to Claim 39, wherein the different signature data elements are generated from the secret key data element, the message data element and a different integer selected from a set having a number of integers equal to a number of the different recording media.

45. (Previously Presented) The media verification system according to Claim 41, wherein the different signature data elements are generated from the secret key data element, the message data element and a different integer selected from a set having a number of integers equal to a number of the different recording media.